МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ

ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Фонды оценочных средств по дисциплине

«ОРГАНИЗАЦИЯ ЗАЩИТЫ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ»

Индикаторы (детализация) компетенции

ОПК.11 Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации
Индикаторы:
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

2. Планируемые результаты обучения

Коды индикаторов компетенций	Планируемый результат
ОПК.11.1	Умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. Знает основные методы политик безопасности АС. Может применить практически
ОПК.11.2	Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Знает типовые уязвимости значимых объектов КИИ. Может предложить решение по защите информации.

3. Спецификация заданий
Задания по дисциплине «Организация защиты значимых объектов критической информационной инфраструктуры» представляет собой перечень примерных вопросов, предлагаемых студентам для письменного анализа, с учетом тем и заданий для контрольных мероприятий, предусмотренных по дисциплине.

Контрольное мероприятие №1.

Рассматриваемые вопросы:

Система нормативных правовых актов по вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации. Объекты и субъекты КИИ. Термины и определения в области обеспечения безопасности КИИ. Государственная система выявления атак на КИИ и противодействия им. Система безопасности значимых объектов КИИ.

1. Государственная система обеспечения информационной безопасности РФ. Основные нормативные документы перечислить и дать краткую характеристику (ФЗ-187, Указ Президента РФ №31с).

Нарисовать схему системы обеспечения информационной безопасности РФ.

2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.
   ГОССОПКА, нарисовать схему взаимодействий с вовлеченными структурами, краткие пояснения.

3. Центры реагирования на компьютерные инциденты в РФ. НКЦКИ, SOC, SERT, их краткая характеристика, взаимодействие с ГОСОПКА, схема. Основные термины и определения.

4. Федеральные государственные органы РФ, осуществляющие полномочия по предотвращению противоправных действий и борьбе с преступлениями в сфере компьютерной информации. Обзор российских SERT.

Работа выполняется в письменном виде. Время выполнения – 1 уч. час.

Контрольное мероприятие №2.

Рассматриваемые вопросы:

Типовые угрозы безопасности информации для ИС, ИТКС, АСУ. Источники угроз безопасности информации. Уязвимость объектов КИИ, классификация уязвимостей. Типовые способы реализации угроз для ИС, ИТКС, АСУ.

1. Объекты КИИ. Объекты защиты. Перечислить типовые значимые объекты КИИ для различных сфер деятельности (производственная, научная, здравоохранение и т.п.). Дать понятие типовых угроз исходя из особенностей деятельности.
2. Типовые уязвимости объектов КИИ. Возможные способы реализации угроз для ЗОКИИ. Внешние и внутренние нарушители, хакерские атаки, сетевое воздействие.
3. Мировая и отечественная практика противодействию угрозам безопасности на объектах КИИ. Компьютерные инциденты. Характеристики типовых угроз для ИС, ИТКС, АСУ. Программные закладки для АСУ.
4. Анализ уязвимостей типового объекта КИИ: код, конфигурация, архитектура значимого объекта КИИ.

Контрольная работа выполняется на занятии в письменном виде. Время – 1 уч. час.

Контрольное мероприятие № 3.

Рассматриваемые вопросы:

Типовые компьютерные инциденты для ИС, ИТКС и АСУ. Порядок категорирования объектов КИИ. Определение объектов КИИ РФ, которые обрабатывают информацию, необходимую для обеспечения критических процессов. Анализ возможных действий нарушителей в отношении объектов КИИ. Оценка возможных последствий инцидентов на объектах КИИ РФ. Показатели критериев значимости. Организационные и технические меры, направленные на блокирование угроз БИ. СЗИ СВТ.

1. Перечислить правила и порядок категорирования объекта КИИ. В каких случаях категорирование не требуется. Для чего формируются комиссии по категорированию, цели и задачи.
2. Существующий порядок определения объекта КИИ. Методы определения критически важной информации. Осуществление управления, контроля или мониторинга критических процессов. Перечислить основные критические процессы в производственной, технологической финансово-экономической и иных сферах.
3. Типовые схемы защиты значимых объектов КИИ. Анализ возможных действий нарушителей и оценка последствий компьютерных инцидентов для ЗОКИИ Российской Федерации.
4. Перечислить и дать краткую характеристику применяемым на объектах КИИ организационно-распорядительным и техническим мерам защиты информации. Провести анализ эффективности (краткий) применяемым средствам защиты информации на объектах КИИ, исходя из требований нормативных документов ФСТЭК России по безопасности информации.

   Время выполнения контрольной работ – 1 уч. час. Работа выполняется в письменном виде.

Контрольное мероприятие № 4.

Рассматриваемые вопросы:

Стадии работ по созданию систем безопасности. Контроль за обеспечением безопасности значимого объекта КИИ.

1. Перечислить и выделить основные элементы разрабатываемой эксплуатационной и организационно-распорядительной документации для различных объектов КИИ и их систем безопасности. Что включают в себя внедряемые организационные меры безопасности на объекте КИИ.
2. Перечислить и дать краткую характеристику последующим этапам внедрения системы безопасности. Установка и настройка СЗИ СВТ, предварительные испытания и опытная эксплуатация объекта КИИ и его системы безопасности.
3. В чем заключается мониторинг событий безопасности и контроль за действиями персонала в значимом объекте КИИ. Внутренний контроль организации работ по обеспечению безопасности ЗОКИИ.
4. Порядок оценки безопасности значимого объекта КИИ.

Работа выполняется в письменном виде. Время выполнения работы – 1 уч. час.

Итоговое контрольное мероприятие.

На итоговом мероприятии студенты представляют индивидуальные учебно-практические работы (УПР), выполненные по материалам курса. В работе каждый студент выполняет анализ и оценку защищенности выбранного объекта как объекта критической информационной инфраструктуры. Проводит все необходимые процедуры по аттестации объекта по требованиям действующих нормативных документов ФСТЭК России и представляет в виде пакета документов (в электронном виде) подтверждающих создание

системы безопасности объекта КИИ. В процессе выполнения УПР преподаватель проверяет правильность выполнения УПР индивидуально у каждого студента поэлементно и всей работы в целом.

Время выполнения работы – в течении изучения курса, итоговое мероприятие – 2 уч. часа.

На итоговом мероприятии каждый студент представляет свою работу преподавателю в электронном виде (на информационном носителе), а также видео презентацию из расчета 5-7 минут.